MODSafe

European Commission
Seventh Framework programme
MODSafe Modular Urban Transport Safety and Security Analysis

Final Hazards Control and Safety Measures Analysis

Deliverable D3.2

Contract No.	218606
Document type	DEL
Version	V1.0
Status	Final
Date	28-08-2012
WP	WP 3
Lead Author	BTSERCS
Contributors	Alstom, Ansaldo, AREVA, Dimetronic, LU, RATP, Thales RSS, TRIT, UVHC, UITP
Description	D3.2
Document ID	DEL_D3.2_BTSERCS_WP3_120823_V0.10
Dissemination level	PU
Distribution	Consortium members and EC

Document History:

Version	Date	Author	Modification [very short description]
V0.1	23-03-2012	BTSERCS	New document
V0.2	29-04-2012	Alstom	Updated by Robert Capel - Alstom
V0.3	09-05-2012	WP3 Team	Reviewed by WP3 partners
V0.4	09-05-2012	WP3 Team	Reviewed by WP3 partners
V0.5	15-06-2012	TRIT	Document format updated.
V0.6	28-06-2012	LUL	Update by Gab Parris - LU
V0.7	2906-2012	RATP	Updated by Timothee Loveluck
V0.8	14-08-2012	BTSERCS	WP10 comments incorporated.
V0.9	22-08-2012	BTSERCS	Incorporate further WP10 comments
V1.0	23-08-2012	Alstom	Incorporate further WP10 comments

Approval:

Authority	Name/Partner	Date
WP responsible	BTSERCS – WP3 Consensus	11-08-2012
EB members	WP10 Consensus	24-08-2012
Coordinator	TRIT	28-08-2012

SEVENTH FRAMEWORK PROGRAMME

Table of Content

List of Tables

1. Summary

This deliverable provides further analysis of any unresolved hazards that were previously outlined in MODSafe Preliminary Hazards Control and Safety Measures Analysis [MODSafe D3.1] matched with the MODSafe Preliminary Risk Analysis [MODSafe D2.1].

The basis for this analysis work is the final MODSafe Risk Analysis [MODSafe D2.3] that has been enhanced from previous deliverable [MODSafe D3.1] to include additional hazards. Additional safety measures have been included in this deliverable where appropriate.

The Annex provides the MODSafe Risk Analysis along with the Safety Measures.

2. References

Reference-ID	Document title, identifier and version
[MODSafe D2.1]	List of Hazards, Preliminary Risk Analysis MODSafe DEL_D2.1_TUD_WP2_091102_V3
[MODSafe D2.3]	Risk Analysis MODSafe DEL_D2.3_TUD_WP2_110531_V2.1
[MODSafe D3.1]	Preliminary Hazards Control and Safety Measures Analysis MODSafe DEL_D3.1_BTSERCS_WP3_110215_V1.0
[MODSafe D4.2]	Analysis of Safety Requirements for Continuous Safety Measures and Functions MODSafe DEL_D4.2_UITP_WP4_110121_V2.0
[MODSafe D4.3]	Analysis of On-Demand Functions MODSafe DEL_D4.3_UITP_WP4_110926_V1.2a
[MODURBAN D80]	Comprehensive Operational, Functional and Performance Requirements MODURBAN DEL D80_v2-5_BVG_WP21_090317
[IEC62290-2]	IEC 62290-2 Railway applications – Urban guided transport management and command/control systems (UGTMS) – Part 2 Functional requirement specification", [2010-06-25]
[GLOSSARY.en]	MODSafe Glossary MODSafe DEL_D10.5_RATP_WP10_101005_V3

3. Terms and Abbreviations

The terms and abbreviations used in this project are explained in the [GLOSSARY.en]. In addition, the following abbreviations are used here:

Term / Abbreviation	Description
EB	Emergency Brake
GOA	Grade of Automation
IEC	International Electrotechnical Commission
M	Mandatory
MODURBAN	FP6 Integrated project full title Modular Urban Guided Rail Systems
NA	Not Applicable, because the safety measure apply only to the technical system and not to operational staff
O	Optional
TSR	Temporary Speed Restriction
WP	Work Package

4. Explanation of the Table

This deliverable (the hazard and risk analysis / hazard log in the annex) is presented in the same format as the MODSafe Risk Analysis [MODSafe D2.3], with corresponding safety functions and Grade of Automation in separate columns.

The analysis performed in this deliverable contains the safety measures parameters described in table 1.

Safety Measures parameter	Description
Generic Safety Measures	Generic Safety Measures
Category of Safety Measure (Technical, Procedural, Maintenance)	Applicable safety measure recommended
GOA	Grade of Automation applicable.
Reference: [MODURBAN D80]	Reference to associated D80 functional requirements if applicable. Otherwise NA.
Reference: [IEC62290-2]	Reference to associated IEC62290-2 functional requirements if applicable. Otherwise NA.
Remarks	Applicable remarks

Table 1: Description of Safety Function parameters

For completeness and to aid in understanding the annex, a small selection of risk parameters inherited from [MODSafe D2.3] are described in table 2. A description of all the risk parameters is out of the scope of this deliverable but the reader should consult reference [MODSafe D2.3] for such information.

Risk parameter	Description
Hazard	• Describes the name of the hazard • The overall understanding of the hazard arises from the tree structure • For each hazard a risk analysis has been undertaken
Hazard cause	• For each hazard possible hazard causes are given
Type of accident	• Assumed accident for each hazard
Possible consequential accident	• For each hazard a level of severity of the possible hazard consequences is estimated • Four levels of severity are assumed • Basis for the estimation are the assumed accident of the hazard
Assumed probability	• Estimation of the frequency of occurrence of the hazardous situation • Does not consider existence of safety measure (initial probability) • Conservative assumptions are taken
Risk Reduction	• Estimation of possible risk reduction • Represent the hazard exposure and/or a possibility to avoid the hazard
Risk	• Estimation of resulting risk • Notation according to EN50126
Remarks	• Contains, if necessary, additional information on the risk parameter

Table 2: Description of Risk parameters

All the sections of the MODSafe Risk Analysis [MODSafe D2.3] have been considered. However, in many cases (especially for section 2, 4, 7 and 9) the corresponding IEC or MODURBAN functions do not apply for this type of hazard as hazard mitigation is not provided by the UGTMS. For example, some hazardous situations are covered by rolling stock design or station design (e.g. use non-inflammable materials).

GOA0 is not within the scope of this analysis as in this mode the driver has full responsibility for the train. The other grades of automation: GOA1a, GOA1b, GOA2, GOA3 and GOA4, are marked as not applicable (NA), mandatory (M) and optional (O).

The safety functions are referenced to the corresponding functional requirements from MODURBAN WP21 D80 [MODURBAN D80] and the standard IEC 62290-2 [IEC62290-2] which is compatible with D80. Non safety functions are excluded from this analysis. However all non-safety functions are listed together with safety functions to demonstrate to the reader that all functions have been considered.

The SIL level allocation is described in the Analysis of Safety Requirements for Continuous Safety Measures and Functions [MODSafe D4.2] with recommendations for certain functions. For on-demand functions, the method is explained in the Analysis of On-Demand Functions [MODSafe D4.3].

All safety functions from [MODSafe D4.2] and [MODSafe D4.3] have been linked to hazards. Traceability is shown in Appendix A.

Finally an 'Estimation of initial risk' column has been added from the Risk Analysis [MODSafe D2.3] in order to include details of the severity of the consequence and the assumed probability of occurrence.

5. Conclusion

For each hazard within the scope of this analysis, it has been possible to find corresponding safety functions in [MODURBAN D80]. Hazards not mitigated by UGTMS safety functions are not covered by the standard [IEC 62290-2].

This deliverable fulfils its objectives to include additional safety measures for any remaining unresolved UGTMS hazards such as non-technical safety measures.

In addition, statistics are provided which demonstrate the ratio of hazards only mitigated by procedures out of the total number of hazards identified; ratio of technical safety measures that have no D80 or IEC62290-2 references, etc…

6. Further Considerations and Recommendations

During the development of deliverables D3.1 and D3.2 it was noted that certain hazards (e.g. 1.1.1.1.3.1.2 or 1.1.1.1.3.2.1 or 1.1.1.1.1.3.2.2) can only be mitigated by operational procedures (P) or maintenance (M) activities. It was agreed that it may not always be appropriate to use human intervention to mitigate a hazard, particularly when such a hazard has a significant consequence and/or a very high level of risk, which therefore requires the human intervention to be highly reliable. Examples of hazards which only have human intervention mitigation (by procedure or maintenance) are listed separately in the Annex. Recommendations to deal with this matter are made below.

The following recommendations are proposed:

1. As noted in section 4 above, there are numerous examples of hazards (some intolerable) that are mitigated by Operational Procedures or Maintenance activities. Indeed, these hazards cannot be covered by UGTMS functions. Then, it is recommended that future research projects examine whether human reliability performance is sufficient to ensure that such hazards are adequately mitigated by reliance upon human intervention, and evaluate whether further technical risk reduction measures could be developed to remove reliance upon human intervention. In addition, Human Factors techniques, such as task analysis, should be utilised to determine whether those Operational or Maintenance procedures which support human intervention in place of technical safety measures are adequate.

2. For all hazards mitigated by human intervention it is also recommended that the Railway Operator conducts a detailed review to ensure that all maintenance procedures are adequate and appropriate levels of training are provided to Operational and Maintenance Staff in order to reduce the probability of human error.

3. It is recommended that future revisions of Railway Safety Norms further consider those intolerable hazards not within the scope of UGTMS that are only mitigated by procedural safety measures.

4. During the project realisation phase, it is also recommended that the Railway Operator conducts a detailed review to ensure that all maintenance procedures are adequate and appropriate levels of training are provided to Operational and Maintenance Staff in order to reduce the probability of human error.

5. For two generic safety measures, MODURBAN D80 functions have been referenced, while no adequate IEC62290-2 function could be associated. It is recommended that future revisions of the IEC62290-2 consider those two issues :

    a. in section 4 (station interior hazards with no train presence) no IEC function has been associated to the safety measure "Supervise other safety related inputs - This function is intended to supervise the detection of hazardous situations by external sensors", while D80 function 5.3.5 has been associated. This is because the hazard is a smoke/fire/etc. in the area of the station platform, and IEC function 5.6.1 only mentions onboard fire/smoke detection devices whereas the detection devices mentioned by MODURBAN are not limited to onboard installation. It is then recommended that future revision of IEC consider also fire/smoke detection devices in station.

    b. The “Load infrastructure data onto MODURBAN” function has no equivalent in IEC62290-2 and should be considered/analysed in future revision of IEC.